On the stability of sets of even type

Zsuzsa Weiner and Tamás Szőnyi *

August 8, 2014

Abstract

A stability theorem says that a nearly extremal object can be obtained from an extremal one by "small changes". In this paper, we prove a sharp stability theorem of sets of even type in $\mathrm{PG}(2,q)$, q even. As a consequence, we improve Blokhuis and Bruen's stability theorem on hyperovals and also on the minimum number of lines intersecting a point set of size at most $q+2\lfloor\sqrt{q}\rfloor-2$; furthermore we improve on the lower bound for untouchable sets.

1 Introduction

The main result of this paper is a stability theorem on sets of even type in $\mathrm{PG}(2,q)$, q even. A stability theorem says that when a structure is "close" to being extremal, then it can be obtained from an extremal one by changing it a little bit.

A *set of even type* S is a point set intersecting each line in an even number of points. By counting the points of S on the lines through a point of S and on the lines through a point not in S, one can see immediately that q must be even. Hence from now on we will assume that $2|q$. Another motivation for studying sets of even type comes from coding theory. Such sets are codewords in the dual code of the code generated by the incidence matrix of $\mathrm{PG}(2,q)$, q

*The authors were partially supported by OTKA grant K 81310. The first author was also supported by the ERC grant DISCRETECONT, No. 227701. At the initial phase of this research the authors were partially supported by OTKA grants T43758 and T49662. In that period they were affiliated with the Computer and Automation Research Institute of the Hungarian Academy of Sciences.

even. The smallest sets of even type, corresponding to codewords of minimum weight, are the *hyperovals*; they have $q+2$ points. Somewhat larger sets of even type were constructed by Korchmáros and Mazzocca [18]. A $(q+t,t)$-arc of type $(0,2,t)$ in $\mathrm{PG}(2,q)$ is a set S of $q+t$ points such that every line meets S in either 0,2 or t points. It is known, see [18], that t has to be a divisor of q. Korchmáros and Mazzocca also conjecture that whenever 4 divides t and t divides q, then there exists a $(q+t,t)$-arc of type $(0,2,t)$. Several constructions can be found in [18] and in Gács, Weiner [14], where it is also proved that the t-secants of a $(q+t,t)$-arc of type $(0,2,t)$ are concurrent. Among the sporadic examples we mention the $(36,4)$-arcs of type $(0,2,4)$ in $\mathrm{PG}(2,32)$ found by Key, McDonough, and Mavron [17]. More examples are given by Limbupasiriporn [20, 21]. Recently, a new infinite class of $(q+t,t)$-arcs of type $(0,2,t)$ was constructed by Vandendriessche for $t=q/4$, see [23]. Planar sets of even type also appear in classifying small weight codewords of the dual code generated by characteristic vectors of hyperplanes of $\mathrm{PG}(n,q)$, see De Boeck [9].

A set of *almost even type* is a point set having only few odd-secants. If we delete a point from a set of even type S then the new point set will have $q+1$ odd-secants, and of course this will also be the case when we add a point to S. If ε points are modified then at least $\varepsilon(q+1-(\varepsilon-1))$ and at most $\varepsilon(q+1)$ odd-secants are obtained. A further motivation to study sets of almost even type comes from small Kakeya-sets in $\mathrm{AG}(2,q)$, q even. If the Kakeya-set is small, then the lines of the Kakeya-set cover almost all points twice, hence in the dual plane they give sets of almost even type. For more details, see [7] and the recent paper [6].

The main result of this paper is the following stability theorem, which will be proved in Section 3.

Theorem 1.1 *Assume that the point set $\mathcal{M}$ in $\mathrm{PG}(2,q)$, $16<q$ even, has δ odd-secants, where $\delta<(\lfloor\sqrt{q}\rfloor+1)(q+1-\lfloor\sqrt{q}\rfloor)$. Then there exists a unique set $\mathcal{M}'$ of even type, such that $|(\mathcal{M}\cup\mathcal{M}')\setminus(\mathcal{M}\cap\mathcal{M}')|=\lceil\frac{\delta}{q+1}\rceil$.*

Let us also interpret this result in terms of codes. A set of points corresponds to a set of lines in the dual plane. Odd-secants correspond to points that are contained in an odd number of lines. Considering the sum of the characteristic vectors of the original lines these are just codewords in the p-ary linear code $(C_1(2,q))$ generated by lines of $\mathrm{PG}(2,q)$, $q=p^h$. If the number of odd-secants is δ in the original setting, then this codeword has

weight (the number of non-zero coordinates) δ. Hence the above result has the following corollary.

Corollary 1.2 *Assume that* $16 < q$, $q = p^h$, $p = 2$. *Let* c *be a codeword in* $C_1(2, q)$ *and let* $w(c)$ *denote the weight of* c. *Then* $w(c) < (\lfloor\sqrt{q}\rfloor + 1)(q + 1 - \lfloor\sqrt{q}\rfloor)$ *implies that* c *is the linear combination of exactly* $\lceil\frac{\delta}{q+1}\rceil$ *different lines. This also implies that such codewords can be more or less explicitly described depending on the configuration of the lines.*

When q is odd, one has to consider multisets, see [15]. There are similar results when p is odd and $h > 1$; when $h = 1$ or 2, we have partial results only. When q is a square, the above corollary is sharp as the Hermitian curve is a codeword with weight $q\sqrt{q} + 1$. For details, see [2].

Earlier general results show that codewords with weight less $2q+(q-1)/2$ were characterised as the linear combination of either one or two lines. (See [12] and [19], where the authors consider codewords arising from projective spaces.) When q is a prime, one must be cautious, since there exist codewords with weight $3q - 3$, which are not the linear combination of three lines. (See [10], 10.3.)

Remark 1.3 A complete arc (maximal w.r.t. inclusion) of size $q - \sqrt{q} + 1$ has $(\sqrt{q}+1)(q+1-\sqrt{q})$ odd-secants, which shows that the bound in Theorem 1.1 is sharp, when q is a square. For the existence of such arcs, see [8], [13], [11] and [16].

Remark 1.4 The famous theorem of Segre (see [22]) says that an arc of size larger than $q - \sqrt{q} + 1$ in PG$(2, q)$, q even, can always be embedded in a hyperoval. A k-arc has $k(q + 2 - k)$ odd secants (they are tangents). For $k > q - \lfloor\sqrt{q}\rfloor + 1$, this is less than $(\lfloor\sqrt{q}\rfloor + 1)(q + 1 - \lfloor\sqrt{q}\rfloor)$. This means that Segre's theorem follows from Theorem 1.1 when q is a square. For q a non-square, the bound coming from Theorem 1.1 is worse (by one) than Segre's bound.

In Section 2, we collected the algebraic background needed for the proofs in this paper. The last two sections contain consequences of our main result.

In Section 4, we improve on Blokhuis and Bruen stability result on hyperovals and as a consequence of that we also improve the folklore bound (see [1]) on the number of lines intersecting a point set of size at most $q+2\lfloor\sqrt{q}\rfloor-2$. Note that the original bound is valid for sets of size at most $2q + 3$. Here

we just state the result for sets of size $q+2$, which is a particular case of Proposition 4.2 for $m=2$.

Proposition 4.2 (for $m=2$) *Let $\mathcal{N}$ be a point set in $\mathrm{PG}(2,q)$, $16<q$ even, of size $q+2$. Assume that the number of lines meeting $\mathcal{N}$ in at least one point is $\binom{q+2}{2}+\nu$, where $\nu<\frac{1}{4}(\lfloor\sqrt{q}\rfloor+1)(q+1-\lfloor\sqrt{q}\rfloor)$. Then there exists a set $\mathcal{N}^*$ of even type, such that $|(\mathcal{N}\cup\mathcal{N}^*)\setminus(\mathcal{N}\cap\mathcal{N}^*)|\leq\lceil\frac{4\nu}{q+1}\rceil$.*

The more general result for sets of size $q+m$, $m\leq 2\lfloor\sqrt{q}\rfloor-2$ can be found in Theorem 4.6. For general m, the condition $q\geq 64$ is imposed but for the particular case $m=2$, it is enough to assume $q>16$.

Untouchable sets were introduced by Blokhuis, Seress and Wilbrink, see [4]. For q even their results were improved by Blokhuis, Szőnyi and Weiner [4]. In Section 5, we further improve the lower bound of the size of untouchable sets in Galois planes of even order.

Theorem 5.3 *The size of an untouchable set U in $\mathrm{PG}(2,q)$, $16<q$ even, having odd lines, is larger than $q+3\lfloor\sqrt{q}\rfloor-7$.*

2 Algebraic background

The proofs in this paper will use certain two variable polynomials. It will turn out that the degree of the greatest common divisor of these polynomials after substituting a value to one of the variables, has nice geometric meaning; and so the next result plays a crucial role in this paper. For details, see [24] and [25].

Result 2.1 *Suppose that the nonzero polynomials $u(X,Y)=\sum_{i=0}^{n}u_i(Y)X^{n-i}$ and $v(X,Y)=\sum_{i=0}^{n-m}v_i(Y)X^{n-m-i}$, $m>0$, satisfy $\deg u_i(Y)\leq i$ and $\deg v_i(Y)\leq i$ and $u_0\neq 0$.*

Furthermore, assume that there exists a value y, so that the degree of the greatest common divisor of $u(X,y)$ and $v(X,y)$ is $n-k$. Denote by n_h, the number of values y' for which $\deg(\gcd(u(X,y'),v(X,y')))=n-(k-h)$. Then

$$\sum_{h=1}^{k-1}hn_h\leq k(k-m).\ \blacksquare$$

3 Proof of the main theorem

Let ℓ_∞ be the line at infinity intersecting the point set $\mathcal{M}$ in an even number of points and suppose that the ideal point (∞) is not in $\mathcal{M}$. Furthermore let $\mathcal{M} \setminus \ell_\infty = \{(a_v, b_v)\}_v$ and $\mathcal{M} \cap \ell_\infty = \{(y_i)\}_i$. Consider the following polynomial:

$$g(X,Y) = \sum_{v=1}^{|\mathcal{M}\setminus\ell_\infty|} (X+a_vY-b_v)^{q-1} + \sum_{(y_i)\in\mathcal{M}\cap\ell_\infty} (Y-y_i)^{q-1} + |\mathcal{M}| = \sum_{i=0}^{q-1} r_i(Y)X^{q-1-i}. \tag{1}$$

Note that $\deg(r_i) \leq i$.

Lemma 3.1 *Assume that the line at infinity contains an even number of points of $\mathcal{M}$. Through a point (y) there pass s odd-secants of $\mathcal{M}$ if and only if the degree of the greatest common divisor of $g(X,y)$ and $X^q - X$ is $q-s$.*

Proof. We only have to show that x is a root of $g(X,y)$ if and only if the line $Y = yX + x$ intersects $\mathcal{M}$ in an even number of points. Since $a^{q-1} = 1$, if $a \neq 0$ and $0^{q-1} = 0$, for the pair (x,y) the number of zero terms in the first sum is exactly the number of affine points of $\mathcal{M}$ on the line $Y = yX + x$, the rest of the terms are 1. The number of ones in the second sum is $q - |\mathcal{M} \cap \ell_\infty|$ or one less, according to the ideal point of the line $Y = yX + x$ being in $\mathcal{M}$ or not. This shows that $g(X,Y)$ is zero for the pair (x,y), when the line $Y = yX + x$ is an even-secant of $\mathcal{M}$. Similarly, one can show that $g(X,Y)$ is not zero for odd-secants of $\mathcal{M}$, hence the lemma follows. ■

Remark 3.2 Assume that the line at infinity is an even-secant and suppose also that there is an ideal point, different from (∞), with s odd-secants. Let n_h denote the number of ideal points different from (∞), through which there pass $s-h$ odd-secants of the point set $\mathcal{M}$. Then Lemma 3.1 and Corollary 2.1 imply that $\sum_{h=1}^{s-1} hn_h \leq s(s-1)$.

Lemma 3.3 *Let $\mathcal{M}$ be a point set in* $\mathrm{PG}(2,q)$*, $16 < q$ even, having $\delta < (\lfloor\sqrt{q}\rfloor+1)(q+1-\lfloor\sqrt{q}\rfloor)$ odd-secants. Then the number of odd-secants through any point is either at most $\lfloor\sqrt{q}\rfloor + 1$ or at least $q - \lfloor\sqrt{q}\rfloor$.*

PROOF. Pick a point $P \neq (\infty)$ with s odd-secants and let ℓ_∞ be an even-secant of M through P. (If there was no even-secant, then the lemma would follow immediately.) Using Remark 3.2, we get that:

$$qs - s(s-1) \leq \delta. \tag{2}$$

Since we do not know anything about (∞), it does not contribute to the left-hand side. It is easy to check that for $s = \lfloor\sqrt{q}\rfloor + 2$ and for $s = q + 1 - (\lfloor\sqrt{q}\rfloor + 2)$, the above inequality is not valid; which shows that $s < \lfloor\sqrt{q}\rfloor + 2$ or $s > q + 1 - (\lfloor\sqrt{q}\rfloor + 2)$. ■

In the subsequent proofs we will use a little modification of the above quadratic inequality (2). Each time we will give the solution (a lower and an upper bound on the valid values). In order to verify that these bounds are valid, as in the above lemma, one should just simply check that the bounding values do not satisfy the given quadratic inequality.

Proposition 3.4 *Let $\mathcal{M}$ be a point set in* $\mathrm{PG}(2,q)$*, $16 < q$ even, having $\delta < (\lfloor\sqrt{q}\rfloor + 1)(q + 1 - \lfloor\sqrt{q}\rfloor)$ odd-secants. Assume that through each point there pass at most $\lfloor\sqrt{q}\rfloor + 1$ odd-secants. Then there is no point through that there pass exactly $\lfloor\sqrt{q}\rfloor + 1$ odd-secants and hence total number of odd-secants δ of $\mathcal{M}$ is at most $\lfloor\sqrt{q}\rfloor q - q + 2\lfloor\sqrt{q}\rfloor + 1$.*

PROOF. Assume to the contrary that $\delta > \lfloor\sqrt{q}\rfloor q - q + 2\lfloor\sqrt{q}\rfloor + 1$. Pick a point P and let ℓ_∞ be an even-secant of $\mathcal{M}$ through P. Assume that there are s odd-secants through P. If there is a point Q on this even-secant through which there pass at least s odd-secants, then choose the coordinate system so that Q is (∞). Then, by Remark 3.2, counting the number of odd-secants through ℓ_∞, we get a lower bound on δ:

$$(q+1)s - s(s-1) \leq \delta.$$

Since $\delta < (\lfloor\sqrt{q}\rfloor + 1)(q + 1 - \lfloor\sqrt{q}\rfloor)$, from the above inequality we get that either $s < \lfloor\sqrt{q}\rfloor + 1$ (hence $s \leq \lfloor\sqrt{q}\rfloor$) or $s > q + 1 - \lfloor\sqrt{q}\rfloor$, but by the assumption of the proposition the latter case cannot occur.

Now we show that through *any* point (not only through those which satisfy the assumption made in the beginning of the proof), there are at most $\lfloor\sqrt{q}\rfloor$ odd-secants. The above argument and Lemma 3.3 show that on each even-secant there is at most one point through which there pass

$\lfloor\sqrt{q}\rfloor + 1$ odd-secants and through the rest of the points there are at most $\lfloor\sqrt{q}\rfloor$ of them. Assume that there is a point R with $\lfloor\sqrt{q}\rfloor + 1$ odd-secants. Since $\delta > \lfloor\sqrt{q}\rfloor + 1$, we can find an odd-secant ℓ not through R. From above, the number of odd-secants through the intersection point of an even-secant on R and ℓ is at most $\lfloor\sqrt{q}\rfloor$. So counting the odd-secants through the points of ℓ, we get at most $(q - \lfloor\sqrt{q}\rfloor)(\lfloor\sqrt{q}\rfloor - 1) + (\lfloor\sqrt{q}\rfloor + 1)\lfloor\sqrt{q}\rfloor + 1$, which is a contradiction; so there was no point with $\lfloor\sqrt{q}\rfloor + 1$ odd-secants.

This means that the odd-secants form a dual $(\delta, \lfloor\sqrt{q}\rfloor)$-arc, hence $\delta \leq (\lfloor\sqrt{q}\rfloor - 1)(q + 1) + 1$, which is a contradiction again; whence the proof follows. ■

Proof of Theorem 1.1 By Lemma 3.3, through each point there pass either at most $\lfloor\sqrt{q}\rfloor + 1$ or at least $q - \lfloor\sqrt{q}\rfloor$ odd-secants. Consider a point through which there pass at least $q - \lfloor\sqrt{q}\rfloor$ odd-secants. If such a point is in $\mathcal{M}$ then delete it, otherwise add it to $\mathcal{M}$. Note that when we modify (delete or add) a point then each odd-secant through that point will become an even-secant and vice-versa. Hence this modification reduces the total number of odd-secants (by at least $q - \lfloor\sqrt{q}\rfloor - (\lfloor\sqrt{q}\rfloor + 1) > 0$) and so we can still apply Lemma 3.3; which shows that through each point in this modified set there pass at most $\lfloor\sqrt{q}\rfloor + 1$ or at least $q - \lfloor\sqrt{q}\rfloor$ odd-secants. Repeat this process (for modifying points with at least $q - \lfloor\sqrt{q}\rfloor$ odd-secants one by one) until there are no points through which there pass at least $q - \lfloor\sqrt{q}\rfloor$ odd-secants. We denote this set by $\mathcal{M}'$. Note that from above through any point of $\mathcal{M}'$ there pass at most $\lfloor\sqrt{q}\rfloor + 1$ odd-secants and also the total number δ' of odd secants of $\mathcal{M}'$ is at most δ. By Proposition 3.4, $\delta' \leq \lfloor\sqrt{q}\rfloor q - q + 2\lfloor\sqrt{q}\rfloor + 1$. *Our first aim is to show that $\mathcal{M}'$ is a set of even type.*

Let P be an arbitrary point with s odd-secants, and let ℓ_∞ be an even-secant through P. Assume that there is another point on ℓ_∞ with at least s odd-secants through it. Then, as in Proposition 3.4, counting the number of odd-secants through ℓ, we get a lower bound on δ':

$$(q + 1)s - s(s - 1) \leq \delta',$$

where either $s < \frac{\delta'+q}{q+1}$ or $s > q + 2 - \frac{\delta'+q}{q+1}$. By the construction of $\mathcal{M}'$, the latter case cannot occur.

As in the proof of Proposition 3.4, by changing the coordinate system, we show that there is no point at all through which there pass at least $\frac{\delta'+q}{q+1}$ odd-secants. On the contrary, assume that T is a point with $\frac{\delta'+q}{q+1} \leq s$ odd-

secants. We choose our coordinate system so that the ideal line is an even-secant through T and $T \neq (\infty)$. Then from above, through each ideal point, there pass less than $s(\geq \frac{\delta'+q}{q+1})$ odd-secants. First we show that there exists an ideal point through which there pass exactly $(s-1)$ odd-secants. Otherwise, by Remark 3.2, we get $2(q-1) \leq s(s-1)$; but this is a contradiction since by Lemma 3.3, $s \leq \lfloor\sqrt{q}\rfloor+1$. Let (∞) be a point with $(s-1)$ odd-secants. Then as before, we can give a lower bound on the total number of odd-secants of $\mathcal{M}'$:

$$(s-1) + qs - s(s-1) \leq \delta',$$

where either $s < \frac{\delta'+q}{q+1}$ or $s > q+2-\frac{\delta'+q}{q+1}$. This is a contradiction, since by assumption, the latter case cannot occur and the first case contradicts our choice of T.

Hence through each point there pass less than $\frac{\delta'+q}{q+1}$ odd-secants. Assume that ℓ is an odd-secant of $\mathcal{M}'$. Then summing up the odd-secants through the points of ℓ we get that $\delta' < (q+1)\frac{\delta'-1}{q+1}+1$, which is a contradiction. So $\mathcal{M}'$ is a set of even type.

To finish our proof we only have to show that $|(\mathcal{M} \cup \mathcal{M}') \setminus (\mathcal{M} \cap \mathcal{M}')| = \lceil\frac{\delta}{q+1}\rceil$. Note that at each step in the process that yields $\mathcal{M}'$ from $\mathcal{M}$, through each point there are at most $\lfloor\sqrt{q}\rfloor+1$ or at least $q-\lfloor\sqrt{q}\rfloor$ odd-secants. Also, observe that this means that if at some stage in this process there is a point with at least $q-\lfloor\sqrt{q}\rfloor$ odd-secants, then through this point there pass at least $q-\lfloor\sqrt{q}\rfloor$ odd-secants of $\mathcal{M}$ (as at each step the number of odd secants though a non modified point can only change by one). Similarly, if at any stage of the process through a non-modified point there are at most $\lfloor\sqrt{q}\rfloor+1$ odd-secants, then through it there pass at most $\lfloor\sqrt{q}\rfloor+1$ odd-secants of $\mathcal{M}$. So we modified precisely the points through which there passed at least $q-\lfloor\sqrt{q}\rfloor$ odd secants of $\mathcal{M}$, hence the number of modified points in total is surely less than $2\lfloor\sqrt{q}\rfloor$. On one hand, if we construct $\mathcal{M}$ from the set $\mathcal{M}'$ of even type by modifying ε points, then $\delta \geq \varepsilon(q+1-(\varepsilon-1))$. Solving the quadratic inequality we get that $\varepsilon < \lfloor\sqrt{q}\rfloor+1$ or $\varepsilon > q+1-\lfloor\sqrt{q}\rfloor$, but from above this latter case cannot happen. On the other hand, $\delta \leq \varepsilon(q+1)$.

From this, the previous inequality and from $\varepsilon \leq \lfloor\sqrt{q}\rfloor$, we get that $\frac{\delta}{q+1} \leq \varepsilon \leq \frac{\delta}{q+1} + \frac{\lfloor\sqrt{q}\rfloor(\lfloor\sqrt{q}\rfloor-1)}{q+1}$. Hence the theorem follows. ■

4 The minimum number of lines meeting a point set

Stability of hyperovals was already studied by Blokhuis and Bruen. A hyperoval is not only nice in the sense that it intersects each line in an even number of points, but it is also extremal in the sense that considering point sets of size $q+2$, a hyperoval intersects the least number, namely $\binom{q+2}{2}$, of lines. The next result shows that a $(q+2)$-set intersecting a bit more than $\binom{q+2}{2}$ lines can always be obtained by modifying a hyperoval a little bit.

Result 4.1 (Blokhuis, Bruen [3]) *Let $\mathcal{H}$ be a point set in $\mathrm{PG}(2,q)$, q even, of size $q+2$. Assume that the number of lines meeting $\mathcal{H}$ in at least one point is $\binom{q+2}{2}+\nu$, where $\nu \leq \frac{q}{2}$. Then $\mathcal{H}$ is a hyperoval or there exist two points P and Q, so that $(\mathcal{H} \setminus P) \cup Q$ is a hyperoval.*

We will improve on the above result. Our improvement is twofold, we will consider point sets with not only $q+2$ points, and also point sets intersecting more lines.

Proposition 4.2 *Let $\mathcal{N}$ be a point set in $\mathrm{PG}(2,q)$, $16 < q$ even, of size $q+m$. Assume that the number of lines meeting $\mathcal{N}$ in at least one point is $\frac{1}{2}(q+m)(q-\frac{m}{2}+2)+\nu$, where $(0 \leq)\nu < \frac{1}{4}(\lfloor\sqrt{q}\rfloor+1)(q+1-\lfloor\sqrt{q}\rfloor)$. Then there exists a set $\mathcal{H}$ of even type, such that $|(\mathcal{N} \cup \mathcal{H}) \setminus (\mathcal{N} \cap \mathcal{H})| \leq \lceil \frac{4\nu}{q+1} \rceil$.*

Proof. First we show that almost all lines meeting $\mathcal{N}$ intersect it in 2 points. Let l_i denote the number of lines intersecting $\mathcal{N}$ in i points. We will do the standard counting arguments to get a lower bound on l_2. That is:

$$\sum_{i=1}^{q+1} l_i = s = \frac{(q+m)(q-\frac{m}{2}+2)}{2} + \nu, \tag{3}$$

$$\sum_{i=1}^{q+1} i l_i = (q+m)(q+1), \tag{4}$$

$$\sum_{i=2}^{q+1} i(i-1) l_i = (q+m)(q+m-1). \tag{5}$$

Calculating $(5) - 3 * (4) - 4 * (3)$ we get

$$\sum_{i:odd} l_i \leq \sum_{i=1}^{q+1} (i-2)^2 l_i = 4\nu, \tag{6}$$

So Theorem 1.1 says that we can modify (add or delete) at most $\lceil \frac{4\nu}{q+1} \rceil$ points of $\mathcal{N}$ so that we obtain a set of even type. The number of modified points is at most $\lceil \sqrt{q} \rceil$. ■

Remark 4.3 The bound on the total number of odd-secants in the above proof is sharp for a point set of size $q+2$ with the property that through each point there pass exactly the same number of 3-secants as 1-secants.

A corollary of the above proposition is that we improve the (folklore) bound on the minimum number of lines intersecting a point set.

Result 4.4 (folklore, see Blokhuis [1]) *Let X be a set of n points in a projective plane of order q. Write $n - 1 = (q+1)a - b$, $0 \leq b \leq q$. Then the number of lines intersecting X is at least $\frac{n}{a(a+1)}(2a(q+1) - n + 1)$. Equality occurs if and only if X is a set of type $(0, a, a+1)$.*

Remark 4.5 Note that, when $m < 2$, Result 4.4 applies with $a = 1$ and so $\nu \geq \frac{1}{2}(-\frac{m}{2} + 1)(q+m)$; hence the assertion of Proposition 4.2 is non-empty if $m \geq -\lfloor \sqrt{q} \rfloor + 1$. This is a generalisation of Segre's theorem (Remark 1.4). Lines meet an arc in 0, 1 or 2 points. In the above proposition we prove that if we have a point set of size at most $q+2$ with the property that the number of lines with intersection number $\neq 0, 2$ is just a little bit more than the 1-secants of an arc of the same size, then we can modify (add or delete) at most $\lfloor \sqrt{q} \rfloor$ points to get a set of even type. Using Result 4.4, when $m \geq 2$, the assertion of Proposition 4.2 is non empty if and only if $a = 2$ in Result 4.4 and so m must be at most $3\lfloor \sqrt{q} \rfloor - 7$. In the next theorem (which will use Proposition 4.2), we will impose an even stronger condition on m, that is $m \leq 2\lfloor \sqrt{q} \rfloor - 2$; which will come from the very end of the proof of the theorem. To do this, we need that $2\lfloor \sqrt{q} \rfloor - 2 \leq 3\lfloor \sqrt{q} \rfloor - 7$; hence $q > 16$.

In the rest of this section we are going to prove the next theorem.

Theorem 4.6 *Let $\mathcal{M}$ be a point set in* $\mathrm{PG}(2,q)$, $16 < q$ *even, of size* $q+m$, $m \leq 2\lfloor\sqrt{q}\rfloor - 2$. *Then the number of lines intersecting $\mathcal{M}$ in at least one point is at least*

- $\frac{1}{2}q^2 + q(\frac{3}{8}m + \frac{3}{4}) - m(\frac{1}{8}m + \frac{3}{4})$, *when m is even,*
- $\frac{1}{2}q^2 + q(\frac{3}{8}m + \frac{7}{8}) - m(\frac{1}{8}m + \frac{3}{2}) + \frac{11}{8}$, *when m is odd.*

Remark 4.7 For a set of size $q+m$, $m \leq 3\lfloor\sqrt{q}\rfloor - 7$, Result 4.4 says that the number of lines intersecting such point set is at least $q^2/2 + q(m/3 + 5/6) - m(m/6 - 5/6)$. Hence we improved the folklore bound for $m \leq 3\lfloor\sqrt{q}\rfloor - 7$ by $q(m/24 - 1/12) + m(m/24 - 19/12)$, when m is even and by $q(m/24+1/24)+m(m/24-14/6)+11/8$, when m is odd. The improvement is roughly $\frac{1}{24}qm$.

Remark 4.8 It follows from Theorem 4.6 that there are no sets of type $(0,2,3)$ of size greater than q but less than $q+m$, with $m \leq 2\lfloor\sqrt{q}\rfloor - 2$.

We will need the next three lemmas to prove our theorem.

Lemma 4.9 *Let $\mathcal{H}$ be a set of even type of size $q+k$ in a projective plane of order q. Then the total number of lines that are not skew to $\mathcal{H}$ is at least* $\frac{1}{2}q^2 + q(\frac{3}{8}k + \frac{3}{4}) - k(\frac{1}{8}k - \frac{3}{4})$.

Proof. Let l_i denote the number of lines intersecting $\mathcal{H}$ in i points. Let us write up the standard equations.

$$\sum_{i=2}^{q+1} i l_i = (q+k)(q+1), \tag{7}$$

$$\sum_{i=2}^{q+1} i(i-1) l_i = (q+k)(q+k-1). \tag{8}$$

Calculating ((7)+(8)), we get

$$\sum_{i=2}^{q+1} i^2 l_i = (q+k)(2q+k). \tag{9}$$

As every line intersects $\mathcal{H}$ in an even number of points, each term of the sum $\sum_{i=2}^{q+1}(i-2)(i-4)l_i$ is non-negative, hence the whole sum is also non-negative. Using this and (9) we get

$$0 \leq \sum_{i=2}^{q+1}(i-2)(i-4)l_i = -(4q+6-k)(q+k) + 8\sum_{i=2}^{q+1} l_i,$$

from which the result follows. ■

Lemma 4.10 *Let $\mathcal{H}$ be a set of even type of size $q+k$ in a projective plane of order q. Add x points to and delete y points from $\mathcal{H}$ to obtain the set $\mathcal{H}'$. Then the total number of lines intersecting $\mathcal{H}'$ in at least one point is at least*

$$\frac{1}{2}q^2 + q(\frac{3}{8}k + \frac{3}{4}) - k(\frac{1}{8}k - \frac{3}{4}) + \frac{x}{2}(q-k+2) - \binom{x}{2} - \binom{y}{2}.$$

PROOF. Through a point not in $\mathcal{H}$ there are at least $(q+1) - \frac{q+k}{2}$ skew lines. By adding x points to $\mathcal{H}$ we add $\frac{x}{2}(q+2-k)$ new lines meeting $\mathcal{H}'$ and only the lines joining two points of the x points added are counted more than once. Hence we have at least $\frac{x}{2}(q+2-k) - \binom{x}{2}$ "new" secants of $\mathcal{H}'$. By deleting y points we "loose" at most $\binom{y}{2}$ of them. ■

Proposition 4.11 *Let $\mathcal{M}$ be a point set of size $q+m$, $m \leq 2\lfloor\sqrt{q}\rfloor - 2$ in a projective plane of order $q \geq 16$, q even. Assume that there exists a set $\mathcal{M}^*$ of even type, such that $|(\mathcal{M} \cup \mathcal{M}^*) \setminus (\mathcal{M} \cap \mathcal{M}^*)| \leq \sqrt{q}+1$. Then the minimum number of lines intersecting $\mathcal{M}$ in at least one point is*

- $\frac{1}{2}q^2 + q(\frac{3}{8}m + \frac{3}{4}) - m(\frac{1}{8}m + \frac{3}{4})$, *when m is even (that is when $\mathcal{M}$ is a set of even type)*
- $\frac{1}{2}q^2 + q(\frac{3}{8}m + \frac{7}{8}) - m(\frac{1}{8}m + \frac{3}{2}) + \frac{11}{8}$,*when m is odd (that is when $\mathcal{M}$ is a set of even type plus one point).*

PROOF. Assume that $|\mathcal{M} \setminus \mathcal{M}^*| = x$ and that $|\mathcal{M}^* \setminus \mathcal{M}| = y$. Let $|\mathcal{M}^*| = q+k$, that is $m = k+x-y$. Then Lemma 4.10 gives us the minimum number of lines intersecting $\mathcal{M}$ in at least one point, that is $f(x,y) = \frac{1}{2}q^2 + q(\frac{3}{8}(m+y-x)+\frac{3}{4}) - (m+y-x)(\frac{1}{8}(m+y-x)-\frac{3}{4}) + \frac{x}{2}(q-(m+y-x)+2) - \binom{x}{2} - \binom{y}{2}$.

It is easy to see that for a given m, and $x, y > 0$ one has $f(x-1,y-1) < f(x,y)$. The change in the value of $f(x,y)$ is $-\frac{1}{2}(q+2-(m+y-x))+(x+y)$. Since $x+y \leq \sqrt{q}+1$, $(m+y-x) \leq \sqrt{q}-1$ and the value of f indeed decreases

if $q \geq 16$. This means that for a given m the minimum of $f(x,y)$ is obtained for $x = 0$ or $y = 0$. Similarly, for a given m, $f(x-2,0) < f(x,0)$, when $x \geq 2$. We also need that $f(0,y-2) < f(0,y)$. These show that for m even, the minimum is obtained for $(x,y) = (0,0)$. For m odd $f(1,0) < f(0,1)$ and the result follows. ■

This proposition is valid for larger m (and with the assumption of $q \geq 64$) as well, but as we mentioned in Remark 4.7 it makes only sense when $m \leq 3\lfloor\sqrt{q}\rfloor - 7$.

Proof of Theorem 4.6: Denote the number of (≥ 1)-secants of the set $\mathcal{M}$ by s and let $s = \frac{1}{2}(q+m)(q-\frac{m}{2}+2)+\nu$. Suppose to the contrary that $s < \frac{1}{2}q^2 + q(\frac{3}{8}m+\frac{3}{4}) - m(\frac{1}{8}m+\frac{3}{4})$, when m is even, and $s < \frac{1}{2}q^2 + q(\frac{3}{8}m+\frac{7}{8}) - m(\frac{1}{8}m+\frac{3}{2}) + \frac{11}{8}$, when m is odd. In both cases $\nu \leq \frac{1}{4}q\lfloor\sqrt{q}\rfloor$ if $m < 2\lfloor\sqrt{q}\rfloor - 2$. Then, by Proposition 4.2, we can modify (add or delete) at most $\frac{4\nu}{q+1} \leq \lceil\sqrt{q}\rceil$ points of $\mathcal{M}$, so that we obtain a set of even type and Proposition 4.11 completes our proof by yielding a contradiction. ■

Remark 4.12 We can explicitly determine the initial segment of the spectrum of the number of lines intersecting a point set S of size $q+m$ in at least one point, if $q+2 \leq |S| \leq q+2\lfloor\sqrt{q}\rfloor - 2$. It follows from Theorem 4.6 (and from Proposition 4.2), that a hyperoval has the minimum number of secants, that is $(q+2)(q+1)/2$. Then the next value is $(q+2)(q+1)/2 + q/2$ that happens when we add one point to a hyperoval. So there is a gap of size $q/2$ in the spectrum. This is followed by the number of secants of a set of even type with $q+4$ points, that is $(q+4)(2q+1)/4$; which yields a second gap of size $q/4$.

Looking at a set of even type with $q+4$ points from a point of it, we see immediately that through each point there should pass exactly one 4-secant, while the rest of the lines are 2-secants. Hence there are $(q+4)/4$ 4-secants and by [14] they pass through one point (nucleus) not in the set. The next value in our spectrum comes from a set of even type with $q+4$ points added an extra point. Depending on whether this extra point lies only on 2-secants or on a unique 4-secant, or it is the nucleus of our set, we get sets where the total number of secants is $(q+4)(2q+1)/4+q/2-1$, $(q+4)(2q+1)/4+q/2$ or $(q+4)(2q+1)/4+3q/4$.

Now let us consider $(q+2)$-sets only. The $(q+2)$-sets with maximum number of 0-secants are hyperovals; they have roughly $q^2/2+3q/2$ 2-secants.

Hyperovals ± 1 points have roughly $q^2/2 + 2q$ (≥ 1)-secants, $(q+4,4)$-arcs of type $(0,2,4)$ minus 2 points have roughly $q^2/2 + 9q/4$ (≥ 1)-secants, hyperovals ± 2 points have roughly $q^2/2 + 5q/2$ (≥ 1)-secants, $(q+4,4)$-arcs of type $(0,2,4)$ plus 1, minus 3 points have roughly $q^2/2 + 11q/4$ (≥ 1)-secants. Then come several examples with approximately $q^2/2 + 3q$ (≥ 1)-secants, including $(q+6,4)$-arcs minus 4 points. As indicated above, the difficulty in going further is the lack of our knowledge on small sets of even type. For example, $(q+6,4)$-arcs are not unique from a combinatorial point of view. It is possible that they don't exist, but probably it is not easy to prove that.

As we do not know too much about sets of even type with at least $q+6$ points, we cannot continue with this calculation.

The study of Kakeya-sets is closely related to the dual of the problem of studying the number of 0-secants of a set. A Kakeya set is the union of lines with the property that there is a line in each direction of $\mathrm{AG}(2,q)$. Dual of a Kakeya-set and the line at infinity is just a $(q+2)$-set with a nucleus (that is a point with only 2-secants through it). It is easy to see that for q even the smallest Kakeya sets come from a dual oval whose (dual) nucleus is the line at infinity. This Kakeya set has size $q(q+1)/2$. Formulated in terms of Kakeya sets, the result of Blokhuis and Bruen [3] says that the next smallest examples have size $q(q+2)/2$. Translated to the (≥ 1)-secant terminology, it is essentially Result 4.1. In [6], Blokhuis, De Boeck, Mazzocca and Storme classify the next smallest example. They come from dual $(q+4,4)$-arcs of type $(0,2,4)$ by deleting two lines. As the previous remark shows, such a result also follows from our work, but for arbitrary $(q+2)$-sets and also we can describe Kakeya-sets up to size $q^2/2 + 3q$ approximately.

5 Untouchable sets in Galois planes of even order

Sets without tangents were introduced by Blokhuis, Seress and Wilbrink [4], who called them *untouchable sets*. It is obvious that an untouchable set has at least $q+2$ points. For q odd, Blokhuis, Seress and Wilbrink proved that the size of a set without tangents in $\mathrm{PG}(2,q)$ is at least $q + \frac{1}{4}\sqrt{2q} + 2$. For q even, the plane $\mathrm{PG}(2,q)$ always has a hyperoval, which is an untouchable set of minimum cardinality; here the question is to find the size of the second smallest untouchable set. Of course, every set of even type is an untouchable

set. The next result gives a lower bound on the possible size of an untouchable set having odd lines.

Result 5.1 [5] *The size of an untouchable set in* $\mathrm{PG}(2,q)$*, q even, having odd-secants, is at least* $q+1+\sqrt{\frac{q}{6}}$.

In this section we will improve on the above bound. First we show that a not too large untouchable set is very close to be a set of even type, hence earlier results of Section 3 apply to such sets.

Lemma 5.2 *Let U be a set without tangents in* $\mathrm{P}G(2,q)$*, q even, $|U| = q+2+\varepsilon$ points. Then the number of odd-secants is at most $\varepsilon|U|/3$.*

Proof. Through any point of U there pass at most ε odd-secants. An odd-secant contains at least 3 points of U, therefore the total number of odd-secants is at most $\varepsilon|U|/3$. ■

Theorem 5.3 *The size of an untouchable set U in* $\mathrm{PG}(2,q)$*, $16 < q$ even, having odd-secants, is larger than* $q+3\lfloor\sqrt{q}\rfloor-7$.

Proof. Assume that $|U| \le q+3\lfloor\sqrt{q}\rfloor-7$. By Lemma 5.2, the number δ of odd-secants of U is less than $(\lfloor\sqrt{q}\rfloor+1)(q+1-\lfloor\sqrt{q}\rfloor)$. By Theorem 1.1, we can construct a set of even type from U by modifying $\lceil\frac{\delta}{q+1}\rceil \ge 1$ points. If P is a modified point, then through P there pass at least $q+1-(\lceil\frac{\delta}{q+1}\rceil-1)$ odd-secants of U. Counting the points of U on the lines through P we get $|U| > 2(q-\lfloor\sqrt{q}\rfloor)$, when $P \in U$, and $|U| > 3(q-\lfloor\sqrt{q}\rfloor)$, when $P \notin U$. This is a contradiction. ■

6 Acknowledgement

We are extremely grateful for the referee's valuable comments and for the thorough reading of our manuscript.

References

[1] A. Blokhuis, Extremal Problems in Finite Geometries, in: *Extremal Problems for Finite Sets* (P. Frankl, Z. Füredi, G. Katona, D. Miklós eds), Bolyai Society Math. Studies **3** (1994), 111–135.

[2] A. Blokhuis, A. Brower, H. Wilbrink, Hermitian unitals are code words, *Discrete Math.* **97** (1991), no. 1-3, 63–68.

[3] A. Blokhuis, A. A. Bruen, The minimal number of lines intersected by a set of $q+2$ points, blocking sets, and intersecting circles. *J. Combin. Theory Ser. A* **50** (1989), no. 2, 308–315.

[4] A. Blokhuis, Á. Seress, H. A. Wilbrink, On sets of points without tangents, *Mitt. Math. Sem. Univ. Giessen* **201** (1991), 39–44.

[5] A. Blokhuis, T. Szőnyi, Zs. Weiner, On sets without tangents on Galois planes of even order, *Designs, Codes and Cryptography* **29** (2003), 91–98.

[6] A. Blokhuis, M. De Boeck, F. Mazzocca, L. Storme, The Kakeya problem: a gap in the spectrum and classification of the smallest examples, *Designs, Codes, and Cryptography*, **72** (2014), 21–31.

[7] A. Blokhuis, F. Mazzocca, The finite field Kakeya problem, eds: M. Grötschel, Gy. O. H. Katona, *Building Bridges, Bolyai Society Mathematical Studies*, **19** (2008), 205–218.

[8] E. Boros, T. Szőnyi, On the sharpness of the theorem of B. Segre, *Combinatorica* **6** (1986), 261–268.

[9] M. De Boeck, Small weight codewords in the dual code of points and hyperplanes in $\mathrm{PG}(n,q)$, q even, *Designs, Codes, and Cryptography*, **63** (2012), 171–182.

[10] M. De Boeck, *Intersection problems in finite geometries*, Ph.D. thesis, Ghent University, Belgium, 2014.

[11] G. Ebert, Partitioning projective geometries into caps, *Canad. J. Math.* **37** (1985), 1163–1175.

[12] V. Fack, Sz. L. Fancsali, L. Storme, G. Van de Voorde, J. Winne, Small weight codewords in the codes arising from Desarguesian projective planes, *Des. Codes Cryptogr.* **46** (2008), no. 1, 25–43.

[13] J. C. Fisher, J. W. P. Hirschfeld, J. A. Thas, Complete arcs on planes of square order, *Ann. Discrete Math.* **30** (1986), 243–250.

[14] A. Gács, Zs. Weiner, On $(q+t,t)$-arcs of type $(0,2,t)$, *Designs, Codes and Cryptography* **29** (2003), 131–139.

[15] A. Gács, T. Szőnyi, Zs. Weiner, On the stability of 0 mod p sets, manuscript.

[16] B. C. Kestenband, A family of complete arcs in finite projective planes, *Colloq. Math.* **57** (1987), 59–67.

[17] J. D. Key, T. P. McDonough, V. Mavron, An upper bound for the minimum weight of the dual codes of Desarguesian planes, *European J. Combin.* **30** (2009), 220–229.

[18] G. Korchmáros, F. Mazzocca, On $(q+t)$-arcs of type $(0,2,t)$ in a Desarguesian plane of order q, *Math. Proc. Cambridge Phil. Soc.* **108** (1990), 445–459.

[19] M. Lavrauw, L. Storme, P. Sziklai, G. Van de Voorde, An empty interval in the spectrum of small weight codewords in the code from points and k-spaces of PG(n,q), *J. Combin. Theory Ser. A* **116** (2009), no. 4, 996–1001.

[20] J. Limbupasiriporn, *Partial permutation decoding for codes from designs and finite geometries*, Ph.D. Thesis Clemson University, 2005, 111 pp. ISBN: 978-0496-95297-7.

[21] J. Limbupasiriporn, Small sets of even type in finite projective planes of even order, *J. Geom.* **98** (2010), 139–149.

[22] B. Segre, Introduction to Galois geometries (ed. J.W.P. Hirschfeld), *Atti Accad. Naz. Lincei Mem. Cl. Sci. Fis. Mat. Natur I* **8** (1967), 133–236.

[23] P. Vandendriessche, Codes of Desarguesian projective planes of even order, projective triads and $(q+t,t)$-arcs of type $(0,2,t)$, *Finite Fields and their Appl.* **17** (2011), 521–531.

[24] Zs. Weiner, *Geometric and Algebraic methods in Galois Geometries*, Ph.D. thesis, Eötvös University, Budapest, 2002., www.cs.elte.hu/∼weiner.

[25] Zs. Weiner, T. Szőnyi, Proof of a conjecture of Metsch, *Journal of Combinatorial Theory Ser. A* **118** (2011), 2066–2070.

Authors address:
Zsuzsa Weiner, Tamás Szőnyi
Department of Computer Science, Eötvös Loránd University,
H-1117 Budapest, Pázmány Péter sétány 1/C, HUNGARY
e-mail: szonyi@cs.elte.hu, weiner@cs.elte.hu

Tamás Szőnyi,
MTA-ELTE Geometric and Algebraic Combinatorics Research Group,
H-1117 Budapest, Pázmány Péter sétány 1/C, HUNGARY

Zsuzsa Weiner
Prezi.com
H-1088 Budapest, Krúdy Gyula utca 12, HUNGARY
e-mail: zsuzsa.weiner@prezi.com